THE KORTEWEG-DE VRIES EQUATION AND A DIOPHANTINE PROBLEM RELATED TO BERNOULLI POLYNOMIALS

Á. PINTÉR AND SZ. TENGELY

Dedicated to Professor Hari M. Srivastava

Abstract. Some diophantine equations related to the soliton solutions of the Korteweg-de Vries equation are resolved. The main tools are the connection with Bernoulli polynomials and the application of certain computational number-theoretical results.

1. introduction

In the paper [12] Fairlie and Veselov obtained a relation of the Bernoulli polynomials with the theory of the Korteweg-de Vries (KdV) equation

$$u_t - 6uu_x + u_{xxx} = 0.$$

This equation has infinitely many conservation laws of the form

$$I_m[u] = \int_{-\infty}^{\infty} P_m(u, u_x, u_{xx}, \ldots, u_m)dx,$$

where P_m are some polynomials of the function u and its x-derivatives up to order m, see [18]. For example,

$$I_{-1}[u] = \int_{-\infty}^{\infty} udx, I_0[u] = \int_{-\infty}^{\infty} u^2dx, I_1[u] = \int_{-\infty}^{\infty} (u_x^2 + 2u^3)dx$$

and

$$I_2[u] = \int_{-\infty}^{\infty} (u_{xx}^2 + 10uu_x^2 + 5u^4)dx.$$

The KdV equation possesses a remarkable family of so-called n-soliton solutions corresponding to the initial profile $u_n(x, 0) = -2n(n+1)\mathrm{sech}^2 x$. For some recent generalizations and applications of the Korteweg-de Vries equation we refer to [15], [14] and [22] and the references given therein.

Using the spectral theory of Schrödinger operators, see [30], Fairlie and Veselov [12] proved that

$$I_k[u_n] = \frac{(-1)^k 4^{k+2}}{2k+3} \sum_{i=1}^{n} i^{2k+3}$$

for $k = -1, 0, 1, \ldots$.

Now let $k \neq l$ be fixed integers with $k, l \in \{-1, 0, 1, 2, \ldots\}$ and suppose that

$$|I_k[u_n]| = |I_l[u_m]|.$$

1991 *Mathematics Subject Classification.* Primary 11D41, 14H45; Secondary 11Y50.

Key words and phrases. Diophantine equations, curves of genus 2, Korteweg-de Vries equation.

Research was supported in part by the Hungarian Academy of Sciences, OTKA grants K75566, K100339, NK101680, NK104208 (Á.P) and OTKA grants PD75264, NK104208, K100339 and János Bolyai Research Scholarship of the Hungarian Academy of Sciences (Sz.T.).

One can ask that for given k and l, how often can these integrals be equal? In other words, what is the cardinality of the set of solutions m, n to the equation

$$\frac{4^k}{2k+3}\sum_{i=1}^{n} i^{2k+3} = \frac{4^l}{2l+3}\sum_{i=1}^{m} i^{2l+3}, \tag{1}$$

where k and l are fixed distinct integers?

Applying some recent results by Rakaczki, see [23] and [24], it is not too hard to give some ineffective and effective finiteness statements for the solutions m and n to equation (1). However, the purpose of this note is to resolve (1) for certain values of m and n including an infinite family of the parameters.

Theorem 1. *For $k=-1$ and $l \in \{0,1,2,3\}$, equation (1) has only one solution, namely $(l,m,n)=(0,24,5)$.*

Theorem 2. *Assume that $k=0$ and l is a positive integer such that $2l+3$ is prime. Then (1) has no solution in positive integers m and n.*

2. Auxiliary results

In our first lemma we summarize some classical properties of Bernoulli polynomials. For the proofs of these results we refer to [21].

Lemma 1. *Let $B_j(X)$ denote the jth Bernoulli polynomial and $B_j = B_j(0), j = 1,2,\ldots$. Further, let D_j be the denominator of B_j. Then we have*
(A) $B_j(X) = X^n + \sum_{i=1}^{j}\binom{j}{i}B_iX^{j-i}$,
(B) $S_j(x) = 1^j + 2^j + \ldots + (x-1)^j = \frac{1}{j+1}(B_{j+1}(x) - B_{j+1})$,
(C) $B_1 = -\frac{1}{2}, B_{2j+1} = 0, j = 1,2,\ldots$
(D) (von Staudt-Clausen) $D_{2j} = \prod_{p-1|2j, p \text{ prime}} p$
(E) $X^2(X-1)^2|B_{2j}(X) - B_{2j}$ (in $\mathbb{Q}[X]$).
(F) $B_j(X) = (-1)^jB_j(1-X)$.

Consider the hyperelliptic curve

$$\mathcal{C}: \quad y^2 = F(x) := x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x + b_0, \tag{2}$$

where $b_i \in \mathbb{Z}$. Let α be a root of F and $J(\mathbb{Q})$ be the Jacobian of the curve $\mathcal{C}$. We have that

$$x - \alpha = \kappa\xi^2$$

where $\kappa, \xi \in K = \mathbb{Q}(\alpha)$ and κ comes from a finite set. By knowing the Mordell-Weil group of the curve $\mathcal{C}$ it is possible to provide a method to compute such a finite set. To each coset representative $\sum_{i=1}^{m}(P_i - \infty)$ of $J(\mathbb{Q})/2J(\mathbb{Q})$ we associate

$$\kappa = \prod_{i=1}^{m}\left(\gamma_i - \alpha d_i^2\right),$$

where the set $\{P_1,\ldots,P_m\}$ is stable under the action of Galois, all $y(P_i)$ are non-zero and $x(P_i) = \gamma_i/d_i^2$ where γ_i is an algebraic integer and $d_i \in \mathbb{Z}_{\geq 1}$. If P_i, P_j are conjugate then we may suppose that $d_i = d_j$ and so γ_i, γ_j are conjugate. We have the following lemma (Lemma 3.1 in [8]).

Lemma 2. *Let $\mathcal{K}$ be a set of κ values associated as above to a complete set of coset representatives of $J(\mathbb{Q})/2J(\mathbb{Q})$. Then $\mathcal{K}$ is a finite subset of $\mathcal{O}_K$ and if (x,y) is an integral point on the curve (2) then $x - \alpha = \kappa\xi^2$ for some $\kappa \in \mathcal{K}$ and $\xi \in K$.*

As an application of his theory of lower bounds for linear forms in logarithms, Baker [1] gave an explicit upper bound for the size of integral solutions of hyperelliptic curves. This result has been improved by many authors (see e.g. [2], [3], [4], [9], [20], [26], [27] and [29]).

In [8] an improved completely explicit upper bound were proved combining ideas from [9], [10], [11], [16], [17], [19], [29], [28]. Now we will state the theorem which gives the improved bound. We introduce some notation. Let K be a number field of degree d and let r be its unit rank and R its regulator. For $\alpha \in K$ we denote by $\mathrm{h}(\alpha)$ the logarithmic height of the element α. Let

$$\partial_K = \begin{cases} \frac{\log 2}{d} & \text{if } d = 1,\, 2, \\ \frac{1}{4}\left(\frac{\log\log d}{\log d}\right)^3 & \text{if } d \geq 3 \end{cases}$$

and

$$\partial'_K = \left(1 + \frac{\pi^2}{\partial_K^2}\right)^{1/2}.$$

Define the constants

$$c_1(K) = \frac{(r\,!)^2}{2^{r-1}d^r}, \qquad c_2(K) = c_1(K)\left(\frac{d}{\partial_K}\right)^{r-1},$$
$$c_3(K) = c_1(K)\frac{d^r}{\partial_K}, \qquad c_4(K) = rdc_3(K),$$
$$c_5(K) = \frac{r^{r+1}}{2\partial_K^{r-1}}.$$

Let

$$\partial_{L/K} = \max\left\{[L:\mathbb{Q}]\ ,\ [K:\mathbb{Q}]\partial'_K\ ,\ \frac{0.16[K:\mathbb{Q}]}{\partial_K}\right\},$$

where $K \subseteq L$ are number fields. Define

$$C(K,n) := 3 \cdot 30^{n+4} \cdot (n+1)^{5.5}\, d^2\,(1+\log d).$$

The following result will be used to get an upper bound for the size of the integral solutions of our equations. It is Theorem 3 in [8].

Lemma 3. *Let α be an algebraic integer of degree at least 3 and κ be an integer belonging to K. Denote by α_1, α_2, α_3 distinct conjugates of α and by κ_1, κ_2, κ_3 the corresponding conjugates of κ. Let*

$$K_1 = \mathbb{Q}(\alpha_1, \alpha_2, \sqrt{\kappa_1\kappa_2}), \quad K_2 = \mathbb{Q}(\alpha_1, \alpha_3, \sqrt{\kappa_1\kappa_3}), \quad K_3 = \mathbb{Q}(\alpha_2, \alpha_3, \sqrt{\kappa_2\kappa_3}),$$

and

$$L = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \sqrt{\kappa_1\kappa_2}, \sqrt{\kappa_1\kappa_3}).$$

In what follows R stands for an upper bound for the regulators of K_1, K_2 and K_3 and r denotes the maximum of the unit ranks of K_1, K_2, K_3. Let

$$c_j^* = \max_{1\leq i\leq 3} c_j(K_i)$$

and

$$N = \max_{1\leq i,j\leq 3} \left|\mathrm{Norm}_{\mathbb{Q}(\alpha_i,\alpha_j)/\mathbb{Q}}(\kappa_i(\alpha_i - \alpha_j))\right|^2$$

and

$$H^* = c_5^* R + \frac{\log N}{\min_{1\leq i\leq 3}[K_i:\mathbb{Q}]} + \mathrm{h}(\kappa).$$

Define

$$A_1^* = 2H^* \cdot C(L, 2r+1) \cdot (c_1^*)^2 \partial_{L/L} \cdot \left(\max_{1\leq i\leq 3} \partial_{L/K_i}\right)^{2r} \cdot R^2,$$

and

$$A_2^* = 2H^* + A_1^* + A_1^* \log\{(2r+1) \cdot \max\{c_4^*, 1\}\}.$$

If $x \in \mathbb{Z}\backslash\{0\}$ satisfies $x - \alpha = \kappa\xi^2$ for some $\xi \in K$ then

$$\log|x| \leq 8A_1^* \log(4A_1^*) + 8A_2^* + H^* + 20\log 2 + 13\,\mathrm{h}(\kappa) + 19\,\mathrm{h}(\alpha).$$

To obtain a lower bound for the possible unknown integer solutions we are going to use the so-called Mordell-Weil sieve. The Mordell-Weil sieve has been successfully applied to prove the non-existence of rational points on curves (see e.g. [5], [7], [13] and [25]).

Let $C/\mathbb{Q}$ be a smooth projective curve (in our case a hyperelliptic curve) of genus $g \geq 2$. Let J be its Jacobian. We assume the knowledge of some rational point on C, so let D be a fixed rational point on C and let $\jmath$ be the corresponding Abel-Jacobi map:

$$\jmath : C \to J, \qquad P \mapsto [P - D].$$

Let W be the image in J of the known rational points on C and $D_1, \ldots, D_r$ generators for the free part of $J(\mathbb{Q})$. By using the Mordell–Weil sieve we are going to obtain a very large and smooth integer B such that

$$\jmath(C(\mathbb{Q})) \subseteq W + BJ(\mathbb{Q}).$$

Let

$$\phi : \mathbb{Z}^r \to J(\mathbb{Q}), \qquad \phi(a_1, \ldots, a_r) = \sum a_i D_i,$$

so that the image of ϕ is the free part of $J(\mathbb{Q})$. The variant of the Mordell-Weil sieve explained in [8] provides a method to obtain a very long decreasing sequence of lattices in $\mathbb{Z}^r$

$$B\mathbb{Z}^r = L_0 \supsetneq L_1 \supsetneq L_2 \supsetneq \cdots \supsetneq L_k$$

such that

$$\jmath(C(\mathbb{Q})) \subset W + \phi(L_j)$$

for $j = 1, \ldots, k$.

The next lemma [8, Lemma 12.1] gives a lower bound for the size of rational points whose image are not in the set W.

Lemma 4. *Let W be a finite subset of $J(\mathbb{Q})$ and L be a sublattice of $\mathbb{Z}^r$. Suppose that $\jmath(C(\mathbb{Q})) \subset W + \phi(L)$. Let μ_1 be a lower bound for $h - \hat{h}$ and*

$$\mu_2 = \max\left\{\sqrt{\hat{h}(w)} \;:\; w \in W\right\}.$$

Denote by M the height-pairing matrix for the Mordell–Weil basis $D_1, \ldots, D_r$ and let $\lambda_1, \ldots, \lambda_r$ be its eigenvalues. Let

$$\mu_3 = \min\left\{\sqrt{\lambda_j} \;:\; j = 1, \ldots, r\right\}$$

and $m(L)$ the Euclidean norm of the shortest non-zero vector of L. Then, for any $P \in C(\mathbb{Q})$, either $\jmath(P) \in W$ or

$$h(\jmath(P)) \geq (\mu_3 m(L) - \mu_2)^2 + \mu_1.$$

The following lemma plays a crucial role in the proof of Theorem 1

Lemma 5. *The integral solutions of the equation*

$$\mathcal{C} : Y^2 = X(X+20)^2(X^2 + 10X + 400) + 140625 \tag{3}$$

are

$$(X, Y) \in \{(0, \pm 375), (-20, \pm 375)\}.$$

Proof of Lemma 5. Let $J(\mathbb{Q})$ be the Jacobian of the genus two curve (3). Using MAGMA we determine a Mordell-Weil basis which is given by

$$D_1 = (0, 375) - \infty,$$
$$D_2 = (-20, 375) - \infty.$$

Let $f = x(x+20)^2(x^2+10x+400)+140625$ and α be a root of f. We will choose for coset representatives of $J(\mathbb{Q})/2J(\mathbb{Q})$ the linear combinations $\sum_{i=1}^{2} n_i D_i$, where $n_i \in \{0,1\}$. Then

$$x - \alpha = \kappa \xi^2,$$

where $\kappa \in \mathcal{K}$ and $\mathcal{K}$ is constructed as described in Lemma 2. We have that $\mathcal{K} = \{1, -\alpha, -20-\alpha, \alpha(\alpha+20)\}$. By local arguments it is possible to restrict the set $\mathcal{K}$ further (see e.g. [5], [6]). In our case one can eliminate

$$\alpha(\alpha+20)$$

by local computations in $\mathbb{Q}_3$. We apply Lemma 3 to get a large upper bound for $\log|x|$ in the remaining cases. A MAGMA code were written to obtain the bounds appeared in [8], it can be found at
`http://www.warwick.ac.uk/~maseap/progs/intpoint/bounds.m`. We obtain that these bounds are as follows

κ	bound for $\log\lvert x\rvert$
1	$6.27 \cdot 10^{307}$
$-\alpha$	$4.48 \cdot 10^{668}$
$-20-\alpha$	$1.89 \cdot 10^{612}$

The set of known rational points on the curve (3) is $\{\infty, (0, \pm 375), (-20, \pm 375)\}$. Let W be the image of this set in $J(\mathbb{Q})$. Applying the Mordell-Weil implemented by Bruin and Stoll and explained in [8] we obtain that $\jmath(C(\mathbb{Q})) \subseteq W + BJ(\mathbb{Q})$, where

$$B = 2^8 \cdot 5^3 \cdot 7^2 \cdot 11^2 \cdot 13^2 \cdot 17^2 \cdot 19 \cdot 31 \cdot 37 \cdot 41 \cdot 43 \cdot 53 \cdot 59 \cdot 71 \cdot 79 \cdot 83 \cdot 89$$

that is

$$B = 4612822330600018820343589 7312000.$$

Now we use an extension of the Mordell-Weil sieve due to Samir Siksek to obtain a very long decreasing sequence of lattices in $\mathbb{Z}^2$. After that we apply Lemma 4 to obtain a lower bound for possible unknown rational points. We get that if (x, y) is an unknown integral point, then

$$\log|x| \geq 2.216448 \times 10^{782}.$$

This contradicts the bound for $\log|x|$ we obtained by Baker's method. $\square$

3. Proofs of the Theorems

Proof of Theorem 1. For $k = -1$ and $l \in \{0,1,2,3\}$ we have the diophantine equations

$$\frac{n(n+1)}{2} = \frac{m^2(m+1)^2}{3}, \tag{4}$$

$$\frac{n(n+1)}{8} = \frac{1}{15} z^2(2z-1) \text{ with } z = m(m+1), \tag{5}$$

$$\frac{n(n+1}{8} = \frac{2}{21} z^2(3z^2-4z+2) \text{ with } z = m(m+1), \tag{6}$$

and

$$\frac{1}{4}\sum_{i=1}^{n} i = \frac{64}{9}\sum_{i=1}^{m} i^9, \tag{7}$$

respectively. One can see that the first three equations are elliptic diophatine equations, thus using the program package MAGMA, subroutines `IntegralPoints` or `IntegralQuarticPoints` is just a straightforward calculation to solve them. In these cases the unique solution is $(l, m, n) = (0, 24, 5)$. The forth equation can be written as follows

$$(2n+1)^2 = \frac{128}{45}(m^2+m-1)(m^2+m)^2(2m^4+4m^3-m^2-3m+3)+1.$$

So we easily obtain a hyperelliptic curve

$$Y^2 = X(X+20)^2(X^2+10X+400)+140625,$$

where $Y = 375(2n+1)$ and $X = 20m^2+20m-20$. By Lemma 5 we have that $X = 0$ or -20. Therefore we have that $m \in \{-1, 0\}$, a contradiction and there is no solution in positive integers of (7). □

Proof of Theorem 2. Now $k = 0$ and $p = 2l+3 \geq 3$ is a prime. From (1) we get

$$p \cdot n^2(n+1)^2 = 3 \cdot 4^{l+1}(1^p + 2^p + \ldots + m^p).$$

Let m and n be an arbitrary but fixed solution. An elementary numbertheoretical argument and Lemma 1 yield that $p|m(m+1)$ and

$$\mathrm{ord}_p\left(\frac{1^p+2^p+\ldots+m^p}{m^2(m+1)^2}\right) = \mathrm{ord}_p\frac{B_{p+1}(m+1)-B_{p+1}}{m^2(m+1)^2} \neq 0.$$

Suppose that $p|m$ and let d the smallest positive integer such that $B_{p+1}(m+1) - B_{p+1} = \frac{1}{d}f(m)m^2(m+1)^2$, and $f(X) \in \mathbb{Z}[X]$. Since $\binom{p+1}{k}$ is divisible by p for $k = 2, \ldots, p-1$ and $B_1 = -1/2$ we have that p is not a divisor of d. The constant term of the polynomial $f(X)$ is $d\binom{p+1}{p-1}B_{p-1}$ and, by von Staudt-Clausen theorem, it is not divisible by p. On the other hand, p is a divisor of m and $f(m)$, we have a contradiction. If $p|m+1$ the we can repeat the previous argument using the fact $f(X) = f(-X-1)$, cf. Lemma 1.

□

Acknowledgement. The work is supported by the TÁMOP-4.2.2.C-11/1/KONV-2012-0010 project. The project is implemented through the New Hungary Development Plan, co-financed by the European Social Fund and the European Regional Development Fund.

References

[1] A. Baker. Bounds for the solutions of the hyperelliptic equation. *Proc. Cambridge Philos. Soc.*, 65 (1969), 439–444.

[2] Yu. F. Bilu. Effective analysis of integral points on algebraic curves. *Israel J. Math.*, 90 (1995), 235–252.

[3] Yu. F. Bilu and G. Hanrot. Solving superelliptic Diophantine equations by Baker's method. *Compositio Math.*, 112 (1998), 273–312.

[4] B. Brindza. On S-integral solutions of the equation $y^m = f(x)$. *Acta Math. Hungar.*, 44 (1984), 133–139.

[5] N. Bruin and M. Stoll. Deciding existence of rational points on curves: an experiment. *Experiment. Math.*, 17 (2008), 181–189.

[6] N. Bruin and M. Stoll. Two-cover descent on hyperelliptic curves. *Math. Comp.*, 78 (2009), 2347–2370.

[7] N. Bruin and M. Stoll. The Mordell-Weil sieve: proving non-existence of rational points on curves. *LMS J. Comput. Math.*, 13 (2010), 272–306.

[8] Y. Bugeaud, M. Mignotte, S. Siksek, M. Stoll and Sz. Tengely. Integral points on hyperelliptic curves. *Algebra Number Theory*, 2 (2008), 859–885.
[9] Y. Bugeaud. Bounds for the solutions of superelliptic equations. *Compositio Math.*, 107 (1997), 187–219.
[10] Y. Bugeaud and K. Győry. Bounds for the solutions of unit equations. *Acta Arith.*, 74 (1996), 67–80.
[11] Y. Bugeaud, M. Mignotte and S. Siksek. Classical and modular approaches to exponential Diophantine equations. I. Fibonacci and Lucas perfect powers. *Ann. of Math. (2)*, 163 (2006), 969–1018.
[12] D. B. Fairlie and A. P. Veselov. Faulhaber and Bernoulli polynomials and solitons. *Physica D*, 152–153 (2001), 47–50.
[13] E. V. Flynn. The Hasse principle and the Brauer-Manin obstruction for curves. *Manuscripta Math.*, 115 (2004), 437–466.
[14] X-L. Gai, Y-T. Gao, X. Yu and L. Wang. Painlevé property, auto-Bäcklund transformation and analytic solutions of a variable-coefficient modified Korteweg-de Vries model in a hot magnetized dusty plasma with charge fluctuations. *Applied Math. Comput.*, 216 (2011), 271–279.
[15] M. S. Ismail. Numerical solution of complex modified Korteweg-de Vries equation by Petrov-Galerkin method *Applied Math. Comput.*, 202 (2008), 520–531.
[16] E. Landau. Verallgemeinerung eines Pólyaschen satzes auf algebraische zahlkörper. 1918.
[17] E. M. Matveev. An explicit lower bound for a homogeneous rational linear form in logarithms of algebraic numbers. II. *Izv. Ross. Akad. Nauk Ser. Mat.*, 64 (2000), 125–180.
[18] R. M. Miura, C. S. Gardner and W. D. Kruskal. Korteweg-de Vries equation and generalizations. II. *J. Math. Phys.* 9 (1968), 1204–1209.
[19] A. Pethö and B. M. M. de Weger. Products of prime powers in binary recurrence sequences. I. The hyperbolic case, with an application to the generalized Ramanujan-Nagell equation. *Math. Comp.*, 47 (1986), 713–727.
[20] D. Poulakis. Solutions entières de l'équation $Y^m = f(X)$. *Sém. Théor. Nombres Bordeaux (2)*, 3 (1991), 187–199.
[21] H. Rademacher. Topics in Analytic Number Theory Springer, Berlin, 1973.
[22] A. S. A. Rady, A. H. Khater, E. S. Osman and M. Khafallah. New periodic wave and soliton solutions for system of coupled Korteweg-de Vries equations. *Applied Math. Comput.*, 207 (2009), 406–414.
[23] Cs. Rakaczki. On the Diophantine equation $S_m(x) = g(y)$. *Publ. Math. Debrecen*, 65 (2004), 439–460.
[24] Cs. Rakaczki. On some generalization of the Diophantine equation $s(1^k + 2^k + \cdots + x^k) + r = dy^n$. Acta Arith., 151 (2012), 201–216.
[25] V. Scharaschkin. *Local-global problems and the Brauer-Manin obstruction.* PhD thesis, University of Michigan, 1999.
[26] W. M. Schmidt. Integer points on curves of genus 1. *Compositio Math.*, 81 (1992), 33–59.
[27] V. G. Sprindžuk. The arithmetic structure of integer polynomials and class numbers. *Trudy Mat. Inst. Steklov.*, 143 (1977), 152–174. Analytic number theory, mathematical analysis and their applications (dedicated to I. M. Vinogradov on his 85th birthday).
[28] P. M. Voutier. An effective lower bound for the height of algebraic numbers. *Acta Arith.*, 74 (1996), 81–95.
[29] P. M. Voutier. An upper bound for the size of integral solutions to $Y^m = f(X)$. *J. Number Theory*, 53 (1995), 247–271.
[30] V. E. Zakharov and L. D. Faddaev. KdV equation is completely integrable Hamiltonian system. *Funct. Anal. Appl.*, 5 (1971), 18–27.

Institute of Mathematics
MTA-DE Research Group "Equations, Functions and Curves"
Hungarian Academy of Sciences and University of Debrecen
P. O. Box 12, H-4010 Debrecen, Hungary
E-mail address: `apinter@science.unideb.hu`

Institute of Mathematics
University of Debrecen
P. O. Box 12, H-4010 Debrecen, Hungary
E-mail address: `tengely@science.unideb.hu`